

SHGetPathFromIDList

The destination string buffer must be long enough to hold the return file path.

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4101 bytes

Attack Category	<ul style="list-style-type: none">• Malicious Input								
Vulnerability Category	<ul style="list-style-type: none">• Buffer Overflow• Unconditional								
Software Context	<ul style="list-style-type: none">• Shell Functions• File Path Management								
Location	<ul style="list-style-type: none">• shlobj.h								
Description	<p>The destination string buffer for SHGetPathFromIDList() must be long enough to hold the return file path. Otherwise, buffer overflows will occur.</p> <p>SHGetPathFromIDList() converts an item identifier list to a file system path.</p>								
APIs	<table border="1"><thead><tr><th>Function Name</th><th>Comments</th></tr></thead><tbody><tr><td>SHGetPathFromIDList</td><td></td></tr><tr><td>SHGetPathFromIDListA</td><td>ASCII implementation</td></tr><tr><td>SHGetPathFromIDListW</td><td>Unicode implementation</td></tr></tbody></table>	Function Name	Comments	SHGetPathFromIDList		SHGetPathFromIDListA	ASCII implementation	SHGetPathFromIDListW	Unicode implementation
Function Name	Comments								
SHGetPathFromIDList									
SHGetPathFromIDListA	ASCII implementation								
SHGetPathFromIDListW	Unicode implementation								
Method of Attack	Buffer Overflow								
Exception Criteria									
Solutions	<table border="1"><thead><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr></thead><tbody><tr><td>When SHGetPathFromIDList() or a variant is called.</td><td>The second parameter, pszPath, must be at least MAX_PATH characters in length.</td><td>Effective.</td></tr></tbody></table>	Solution Applicability	Solution Description	Solution Efficacy	When SHGetPathFromIDList() or a variant is called.	The second parameter, pszPath, must be at least MAX_PATH characters in length.	Effective.		
Solution Applicability	Solution Description	Solution Efficacy							
When SHGetPathFromIDList() or a variant is called.	The second parameter, pszPath, must be at least MAX_PATH characters in length.	Effective.							
Signature Details	<pre>BOOL SHGetPathFromIDList(LPCITEMIDLIST pidl, LPTSTR pszPath);</pre>								

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

Examples of Incorrect Code	<pre>TCHAR pszPath[15]; // Buffer too small [...] // get an item identifier list from somewhere if (! SHGetPathFromIDList(pidl, pszPath)) { /* handle error */ }</pre>					
Examples of Corrected Code	<pre>TCHAR pszPath[MAX_PATH]; // Buffer correctly sized [...] // get an item identifier list from somewhere if (! SHGetPathFromIDList(pidl, pszPath)) { /* handle error */ }</pre>					
Source Reference	<ul style="list-style-type: none"> • http://archives.neohapsis.com/archives/nbugtraq/2000-q1/0097.html 					
Recommended Resources	<ul style="list-style-type: none"> • MSDN reference for SHGetPathFromIDList³ • MSDN information on The Shell Namespace and item ID lists⁴ • MSDN information on Working with Item ID Lists⁵ 					
Discriminant Set	<table border="1"> <tr> <td>Operating System</td> <td> <ul style="list-style-type: none"> • Windows </td> </tr> <tr> <td>Languages</td> <td> <ul style="list-style-type: none"> • C • C++ </td> </tr> </table>	Operating System	<ul style="list-style-type: none"> • Windows 	Languages	<ul style="list-style-type: none"> • C • C++ 	
Operating System	<ul style="list-style-type: none"> • Windows 					
Languages	<ul style="list-style-type: none"> • C • C++ 					

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>